Information Networks in

The Army After Next

A MONOGRAPH

by

Major Francis J. Huber

Signal Corps

School of Advanced Military Studies

United States Army Command and General

Staff College

Fort Leavenworth, Kansas

First Term AY 99-00

SCHOOL OF ADVANCED MILITARY STUDIES

MONOGRAPH APPROVAL

Major Francis J. Huber

Title of Monograph: *Information Networks in the Army After Next*

Approved by:

Robert H. Berlin, Ph.D. — Monograph Director

COL Robin P. Swan, MMAS — Director, School of Advanced Military Studies

Philip J. Brookes, Ph.D. — Director, Graduate Degree Program

ABSTRACT

INFORMATION NETWORKS IN THE ARMY AFTER NEXT by MAJ Francis J. Huber, SC, 41 pages.

The Army After Next envisions an Army which has two key attributes, Knowledge and Speed. Speed is the ability of weapons systems to move faster on the battlefield. Knowledge is the ability of forces throughout the battlefield to see themselves and the enemy through the advantages of Sensors, computers and the networks that connect them. In order for this vision to become a reality the sensors, computers and weapon control systems of the Army After Next must have a robust, reliable and secure data network to interlink them or the envisioned advantages of this force will be abrogated.

This monograph examines the direction of the U.S Army at the end of the twentieth century through its Force XXI initiates, the Joint community in the Joint Tactical Radio System program, the U.S. Marine Corps in their Operational Maneuver from the Sea and the U.S. Navy with the High Speed MObile interNET (MONET). It also examines two commercial alternatives, Ricochet Micro Cellular and Cellular Packet Data (CPD) for their applicability and leverage for designing the Intelligent Information Grid for the Army After Next. The focus of the examination is on the applicability of the systems for echelons at Brigade and Below (EBB). Providing data communications networks at this echelon presents the greatest challenge to the Army After Next because of the lethal and mobile nature of the brigade combat environment in the twenty first century.

The study concludes that the current U.S. Army architecture, Force XXI, is inadequate to meet the challenges of the Army After Next. However, the Joint Tactical Radio System (JTRS) as it is currently envisioned with some incorporation of the technologies presented by the Ricochet commercial network does present a superior alternative for the Intelligent Information Grid (I^2G).

Table of Contents

I. Introduction

To achieve land force dominance in 2025 the U.S. Army has identified two required capabilities, “Knowledge” and “Speed”.[1] Speed is described simply in terms of having faster weapons systems and logistics vehicles. Knowledge is summation of situational awareness, both friendly and enemy, relevant to battlespace effectiveness. The warfighter requires a data network which can provide information when it is needed, where it is needed with a reasonable assurance that the data has not been altered or intercepted.[2] Finding the right systems to build this data network or “Information Grid” will be a key to the success of the Army After next in the full spectrum of conflict envisioned in the Joint Vision 2010.

The data communications architecture of the army is the underpinning of the entire structure of the Army After Next. Without the ability to provide the data connectivity between the Army After Next computer systems the advantages of knowledge and speed will be abrogated. If an adversary can nullify the United States Army’s ability to move data across the battlespace he will effectively neutralize the technological advantages of the Army After Next. Therefore the information grid must be sufficiently robust and secure to resist any such attacks. At the same time the network must reduce the manpower required and the weight of the

Army’s current communication systems, especially at echelons of brigade and below. To produce communications systems which are more effective, lighter, and easier to operate and manage will be a significant challenge facing the Army After Next.[3]

Examining the Army’s road to Joint Vision 2010 it is important to understand where the Army is in 1999 with digitization in order to better understand its destination. The Force XXI efforts provide a baseline demonstrated during various Advanced Warfighting Experiments (AWE) as capable of providing the information necessary to support battlefield digitization. However, the communications systems of Task Force XXI have been cobbled together to provide a minimum level of capability.[4] This minimum level will be inadequate as the force moves to support Joint Vision 2010. A faster, lighter, more secure, reliable, and easier to manage system will be required to support a rapidly changing battlespace with systems entering and leaving geographic areas rapidly. The system must be able to adapt to these changes as they occur. The system must provide both network and transmission security to protect the system from the various threats. If knowledge is the key lever in Joint Vision 2010 then the security needed to protect that component will be of paramount importance.

The systems of the future should also be sufficiently technologically mature to provide confidence in the ability to field an operational system as scheduled. The system must posses the ability to move the large volumes of data that will be required for true situational awareness quickly across the battlefield.

In the examination of possible directions for the Army beyond 2010 it is important to address not only the directions being taken by the joint community and the services but also to examine the trends of the commercial market. Utilizing Commercial off the Shelf (COTS) engineering, architectures, and equipment significantly reduces both developmental costs and risks as those costs can then be borne by the industry rather than by the US Government. Echelons above Division (EAD) communications units in DoD have successfully used COTS equipment and software in many applications.[5]

II. Evaluation Criteria

A fundamental attribute enabling the United States Army to fight as a Joint team is its ability to communicate not only internally, but with its sister services. This is expected to remain a procurement focus for the Army as it moves to Force XXI and beyond.[6] Army systems must be interoperable with other systems in the Army and with systems in sister services. The compatibility must be transparent and robust. These systems will need to be interoperable both at the data link layer and at the application layer. Interoperability will facilitate the creation of a “systems of systems” which will permit the aggregation of various forms of permitting the commander to rapidly see all relevant information.[7] To support this commonality the Army has defined expansions of the DoD standards and developed programs to implement the standards.

The Joint Technical Architecture - Army (JTA-A) is the Army’s implementation of the DoD Joint Technical Architecture. The JTA-A provides the basis for which all information technology solutions must be evaluated. The objectives of the JTA-A are clearly stated in its’ introduction.

> The first and foremost objective is to provide the foundation for a seamless flow of information and interoperability among all tactical, strategic, and sustainment/combat support systems that produce, use, or exchange information electronically. The second objective is to mandate standards and guideline for system development and acquisition that will dramatically reduce cost, development time, and fielding time for improved systems. The third objective is to communicate to industry the Army’s intent to consider open system products and implementations.[8]

The first criterion that should be used to evaluate any solution for a force based on knowledge and speed is adaptability. Adaptability is the attribute of a network that allows it to continue functioning as the network or environment changes. A network designed to operate in the highly lethal environment of 2025 must be able to continue to function even after the loss of a significant number of stations or nodes. The network should adapt and change itself as various forces move in and out of a particular geographic area. The network must be able to defend itself from various forms of electronic and information “attacks”.[9] These capabilities will enhance the physical security of the network.

Security will be a key attribute of the information networks for the Army After Next. As the overall level of technological availability and competence grows world wide so will the threats to information networks.[10] The Army After Next wargames have demonstrated that there are significant vulnerabilities in current architectures that future opponents may attempt to take advantage of.[11] Security is a complex criterion that has at least nine major sub elements.

The purpose of a security architecture is not to make a system more difficult to use, it is to ensure the information on the network is accurate, accessible and secure.[12] The attributes that support that functionality are defined in the DoD Goal Security Architecture (DGSA). The specific security services discussed in the JTA-A are authentication, access control, data integrity, data confidentiality, non-repudiation, availability, security audit and key management.[13]

Confidentiality is the protection of transmitted data from being read by an unintended party and protecting data from analysis. Authentication is the assurance that the source of a message is who it claims to be, and ensuring that continuing communications are not from a third party masquerading as either of the original two parties. Integrity has two attributes, one is ensuring that a given data stream is complete and accurate, and the second is ensuring that the data connection between two parties remains available. Nonrepudiation is a mechanism by which a receiver can prove that a message did in fact originate from the sender, and the sender can verify that the receiver did in fact receive the message. Access control is ability to limit access to either systems, data or communications links. Availability is ensuring that data and communications links are available when required.[14] Security audit and key management or additional DoD standards required to support classified architectures.

Key Management is a service that relates to data and communications encryption, and is required for writer to reader secure transactions. Security audit is a service which monitors network and data functions to record individual actions and assist in identifying attempted network penetrations or compromises.

Technological Maturity is a third criterion involving two key attributes. The first is that the technology has been implemented in a production environment as opposed to either concepts or prototype systems in a laboratory setting. The second is that the technology is sufficiently mature in that it has been adopted as a standard by a recognized standards body.

The fourth criterion, bandwidth is a combination of two measures. One is, what the maximum data transfer rate of the network, typically measured in bits per second, and the second is the effects of stress, such as peak data loads, or communications noise on the ability of the network to adapt and continue to pass critical data in a timely manner.[15]

III. Force XXI and the First Digitized Division

As Army planners began to prepare for the 21st century they realized that the unique attribute that would be possessed by dominant forces in that century would be the capabilities presented by information technologies. To rapidly begin leveraging these technologies the Army began a series of Advanced Warfighting Experiments to design and equip a force which would be able to use information to dominate the battlefield. However, Force XXI was about more than just equipment, the Force XXI initiatives were also about doctrine, organizations, training and sustainment. Force XXI uses technology to increase the lethality and effectiveness of weapons and support systems on the battlefield.[16]

A key to achieving the increased lethality and effectiveness promised by Force XXI is the concept of distributed operations. Operations are distributed in space and yet synchronized in time in order to achieve simultaneity and massed effects. This requires dispersed systems which can be synchronized and employed to a common purpose in time and space more rapidly than an adversary can react.[17] An underlying component of this capability is the ability to transmit information across the battlefield to all weapons and sustainment systems in a timely and seamless manner. Information will have to be transmitted quickly, reliably and in large volumes in order to make this concept work.[18] This data network, or internet, is the linchpin in the ability of Force XXI to achieve information dominance as part of the joint team.

The Tactical Internet is the portion of the Force XXI network that supports data communications for the Army Battle Command System (ABCS) at Echelons Brigade and Below (EBB).[19] The tactical internet at EBB consists of four major hardware systems, The Enhanced Position Location and Reporting System (EPLRS), Near Term Digital Radio (NTDR), Combat Net Radio (CNR) Single Channel Ground Airborne Radio System (SINCGARS) System Improvement Program (SIP), and the Mobile Subscriber Equipment Tactical Packet Network (MSE-TPN). Each of these systems provides functionality to the Force XXI tactical Internet.

The lowest level networks in the hierarchy of the Force XXI tactical internet is the SINCGARS SIP with Internetworking Controller. This is an enhanced version of the SINCGARS radios currently in the force that contain an improved data communications ability and a built in internet controller. The SINCGARS SIP provides data communications for an individual Force XXI Battle Command Brigade and Below (FBCB2) computer to the battalion level network. The SINCGARS SIP is capable of a maximum data transmission rate of 9600 bps.[20] The SINCGARS SIP network is used to send and receive situational awareness data to the Company Net Control Station (NCS). The NCS is equipped with an EPLRS radio to connect that data to the Battalion System Integration Van (SIV).

The EPLRS has been described as the “heart” of the tactical internet. In the point to point mode it can achieve data rates of up to 57 kilobits per second.[21] This permits the redistribution of Situational Awareness and Command and Control information from the company nets to the Battalion and Brigade Tactical Operating Centers (TOC). It is this capability that allows the Battalion and Brigade commanders to “see the battlefield” and to distribute timely command and control information by way of the “common relevant picture”.[22] However, even the 57 kb/s capability of the EPLRS system is inadequate to disseminate all of the required data between TOC’s.

The Near Term Digital Radio (NTDR) will provide the data link between TOC’s. The NTDR is a data only radio capable of operating at a maximum data rate of 288 kb/s and is used to interconnect Brigade and Battalion TOC’s.[23] The NTDR facilitates the large volumes of data necessary between the Command and Control headquarters in Force XXI without having to utilize fiber optic cables or other physical infrastructure. This allows TOC’s to establish data communications with each other without the long set up times and manpower requirements of cable installations. The true lethality of Force XXI comes from improved synchronization at all levels.

The Mobile Subscriber Equipment Tactical Packet Network (MSE-TPN) provides the data and voice links from the Brigade TOC’s to the Division Command Posts. The MSE is capable of providing data links of up to 256 kb/s when equipped with the High Speed Multiplex (HS-MUX) upgrade.[24] The MSE network also provides the legacy voice network to the Brigade TOC’s and Brigade Support Areas. While this network utilizes currently available technologies it does contain significant weaknesses.

The Force XXI data network degrades the ability to fully leverage the capabilities of Force XXI due to the tactical internets limitations of a static network, low data rates and lack of security. The Tactical Internet is based upon commercial technologies originally designed to operate in a static environment.[25] Because the networks are built in company, battalion and brigade nets these networks must remain in a static configuration during an operation. During the National Training Center Advanced Warfighting Experiment task organizations could only be changed during the 12-24 hour “change of mission” time period.[26] This means that units cannot change task organization or leave the geographic vicinity of their parent unit without causing significant havoc within the data network and possibly a complete loss of data connectivity. The second significant problem is the inability of the tactical internet to move all of the data that is desired down to the company, platoon and squad level. The bandwidth of the network is insufficient to transmit changing situation templates and graphics in a timely manner during an operation.[27] The final weakness of the system is that it does not possess the capability to perform end to end security functions. The security architecture relies upon individually encrypted links and terminal access controls. The network is operated at a SECRET high level where all of the information is essentially accessible throughout the network. While some network management tools are present to detect security events they are limited in their functionality.[28] As technologies mature these limitations should be reduced in magnitude.

IV. Joint Tactical Radio System

The Joint Tactical Radio System (JTRS) is a DoD program designed to provide a common radio family to all services to meet the future radio requirements of all three services. The JTRS program was started as a result of a Defense Quadrennial Review requirement to consolidate radio programs among all of the services. This requirement grew from continuing problems with establishing intraservice communications links at critical times.[29] The JTRS is intended to replace most of the radio components of the Force XXI tactical internet including SINCGARS-SIP, EPLRS and NTDR.[30] As such it is being designed with a broad range of capabilities in order to meet the needs of the Joint Force in Joint Vision 2010, while utilizing as much commercial technology as possible.

The JTRS is currently in development and has not yet been prototyped, so its compliance with standards is difficult to measure. The JTRS Operational requirements document mandates compliance with the Joint Technical Architecture (JTA), the National Airspace Systems architecture, North Atlantic Treaty Organization Standardization Agreements (NATO STANAGS) and the Defense Information Systems Agency (DISA) “profile of standards” for information technology.[31] At the same time the system has competing requirements for backwards compatibility with many different service radio systems. If the threshold version of the radio is able to meet all of the standards and the performance requirements it will be a standards compliant radio.

The Joint Tactical Radio System is intended to achieve the requirement for compliance with a wide variety of standards and frequency bands through the use of an open systems architecture and software reprogramable components. In fact the open systems architecture, and “modular, scaleable and flexible in form factor” requirement is defined as a “Key Performance Parameter” which must be met by any system proposed for adoption as the Joint Tactical Radio System.[32] The JTRS is subdivided in the Mission Needs Statement (MNS) into two separate subsystems, the radio system and the network. The radio system is intended to meet many of the challenges currently facing tactical radio systems. This includes the ability to pass increasing amounts of data in a bandwidth constrained environment, while at the same time decreasing overall space, weight, power and cost.[33] The radio system must be able to adjust power and bandwidth requirements dynamically in order to minimized demands for constrained resources, such as the frequency spectrum, while at the same time providing the bandwidth when it is needed. Bandwidth is a key determinate in the functionality of the networked portion of the radio system.

The networked portion of the radio must be able to perform dynamic intranetwork and inter-network routing for data transport, and must be able to serve as a gateway between the JTR network and other military Internet Protocol Networks.[34] Specifically the system has a requirement to be able to reconfigure a 150 terminal network within 15 minutes, this is distinct from the current Force XXI Tactical Internet which typically requires 12 to 24 hours to reconfigure a network.[35] This ability to dynamically reconfigure the network enhances the capabilities of the Joint Force significantly and allows a rapid reorganization "on the fly".

To permit the rapid fielding of the radio system the requirements have been broken down into "threshold" and "objective" requirements that are intended to be met over time as the radio matures. The threshold networked system is required to have an embedded GPS, capable of simultaneous voice and data communications, and capable of data rates of up the 16 kb/s. While this is an improvement over the SINCGARS-SIP data rate of 9.6 kb/s it is still significantly less than the EPLRS 57 kb/s capability. As a result the Army migration plan calls for a phased migration where the threshold system replaces the current SINCGARS-SIP radios and the later objective or “wideband” radio replaces the EPLRS and NTDR radio systems.[36] Achieving the networked version of the radio at the 57 kb/s capability has significant technical challenges.

The first challenge is the identification of a modulation technique that will permit the passing of 57 kb/s of data inside the current VHS band. The current SINCGARS channel spacing provides a 25 KHz channel band, for frequency shift keying (FSK) the maximum theoretical baud rate would be one half of the channel bandwidth or 12.5 kb/s second. If a phase shift modulation is then applied on top of this the maximum data rate is the phase shift rate times the baud rate. Current technology has a maximum of Quadrature phase shift keying (four phase shifts per cycle) which produces a maximum theoretical data rate of 50 kb/s. Due to the problems of fading and distortion which occur in the VHF band the current state of the art is limited to a practical level of about 16 kb/s. One study recommended the usage of the Microwave band, specifically 902-928 MHz, in order to overcome the propagation problems and provide a greater channel bandwidth to support higher data rates.[37] The engineering challenge to this is that it requires a radio that can simultaneously operate in the VHF band for backwards compatibility and operate in the microwave band to achieve the higher data rates required for the Army After Next.

A second challenge facing the JTRS is the development of routing protocols that support dynamic reconfiguration of a network. A router network uses two kinds of protocols to build routing tables which are used to forward packets in a network. The first type is the exterior gateway protocol. This is the protocol which a network of routers uses to advertise to another network of routers what is the entrance route for its internal subnets. The JTA-A mandates the use of the Border Gateway Protocol -4 (BGP-4) as the gateway router protocol. The other protocol used by a router network is the interior gateway protocol. The interior protocol is used by the routers inside a network to determine where to forward packets within the network and where to forward packets for external networks. The interior protocol mandated by the Joint Technical Architecture is the Open Shortest Path First (OSPF) v2 protocol. Both of these protocols are designed for relatively static networks with high bandwidth connections between the core routers. The overhead required to reconfigure a complex network based on these protocols was part of the reason for the long reconfiguration times experienced by Task Force XXI during the Advanced Warfighting Experiments.

Supporting the requirement for the network to reconfigure itself with 15 minutes newer internal routing protocols have been proposed, Maximum Forward Routing (MFR) and Just in Time Transceiver Endpoint Route (JITTER). The JITTER protocol requires a node to become active only if it hears a packet. Each node then only tracks the nodes that it can hear from, or transmits to. This mode of operation reduces power utilization and supports the requirement for the network to be able to operate in “listening silence” conditions. The MFR protocol utilizes a broadcast channel to construct and broadcast a table of all of the nodes in the network and their locations. While this somewhat improves the network data performance it has been found to degrade the call set up performance and represents a security risk in that each node will have a table of the locations of all of the other nodes stored in memory. If a node can be captured or compromised this table could theoretically be used to target the nodes.[38] If a protocol like JITTER is implemented as part of the threshold JTRS the system will be better able to meet the dynamic reconfiguration requirements, though changes to the JTA-A will have to be made to accommodate the newer protocols. This may also cause the system to use a protocol which is not in wide use in the commercial sector.

Based upon the number of requirements in the operational requirement document dedicated to security the JTRS should provide a relatively high degree of security. The threshold system is required to be capable of point to point (link) security, over the air rekeying (OTAR) and remote exclusion and zerioizing of compromised terminals. The networked version is required to be able to provide security for a secret high network and the ability to detect and alert the operator to the presence of viruses during initialization.[39] The objective version of the JTRS has requirements that resolve those features that are not implemented in the threshold version such as private key infrastructure for end to end security and multi level security.

V. Navy MONET

Like the JTRS the Navy High Data Rate Mobile Internet (MONET) is essentially a concept, however it is also a test bed in a laboratory setting so it is possible to arrive at an initial understanding of its conceptual design and compliance with standards and requirements. Further as concepts in MONET have been found to be technologically mature and desirable they have been gradually incorporated into the Navy’s IT 21 initiative so that some of the test bed components are also deployed in an operational environment.

The purpose of MONET is to extend the Defense Information Systems Network form shore to ships at sea. The target data rate for a link is the commercial 1.544 megabit data rate (T1). This is an aggregate level link which caries voice, data, video teleconferencing, radar and weapons data and any other routine tactical traffic. The link must be of high enough quality to support all of the applications that are running over it.[40] This provides the requirements base for designing the test network.

The test bed is configured to simulate a deployed network of four ships which represent either carriers or support ships deployed as part of Naval battle groups. The local sites are interconnected using Microwave line of site radios operating in the Super High Frequency (SFH) band representing ships within a battle group operating within electrical line of site of each other. The other sites are interconnected utilizing Satellite Communications (SATCOM) links operating in various commercial bands such as the Ku band with a data rate of 44.7 Mb/s.[41] During the satellite testing it was determined that delay had a negligible effect on network performance and that error rates up to 10^{-6} also had a negligible impact network performance. At error rates greater than 10^{-6} the ATM switches began to have difficulty maintaining their protocols.

The ATM protocols are recognized by the JTA-A for most data applications. Standards for Constant Bit Rate (CBR) applications and for cell prioritization for congestion avoidance are designated as emerging standards.[42] It is unclear from the information available whether the ATM switches utilized in the test bed implement the emerging standards. Presumably the fielded version of the system would implement the mandated standards. Also one of the tested end user applications, Video Teleconferencing, did use an approved standard. The specific application tested is the Picturetel PCS-Live 100. This application suite implements the H.320 video teleconferencing standard which is recognized for medium data rate video teleconferencing applications. The largest clear deviation from the JTA-A is the use of Layer 2 Bridging for connecting the shipboard networks instead of Layer 3 routing. This is a deviation from the JTA-A which clearly mandates the use of Internet Protocol (IP) based routing.[43] The lack of any routing data makes some of the performance characteristics of the network difficult to evaluate.

Clearly this network is intended for use in a relatively static network. Once a satellite link is established to a ship at sea it could be maintained for an indefinite period of time. The SHF links would also be relatively static in that battle groups do not appear to change task organization frequently once they are at sea. Further the equipment form factors are not significantly constrained in that this network appears to be designed for deployment exclusively on larger battle group vessels. The lack of design consideration for dynamic reconfiguration gives it a serious liability as a potential candidate for a data network for the Army After Next.

MONET’s primary strength is in its bandwidth capability. The minimum data rate of 1.544 Mb/s is significantly higher than most of the data rates considered for the Army after next systems. This would make this system an ideal candidate to support relatively static headquarters and facilities where minimal network reconfiguration would be required and most moves are planned well in advance. The system is forward thinking in that it merges the functionality of voice, data and video into a single switched network instead of requiring parallel, resource intensive networks for each service.[44]

By using a large degree of Commercial of the Shelf (COTS) equipment the overall technological maturity of the network is high. Some specific work arounds had to be utilized to compensate for the areas where ATM is still relatively immature, specifically the integration of constant bit rate (CBR) applications such as voice and VTC over ATM. Since standards for CBR signaling and controls have been adopted since the initial MONET report was completed this specific problems should be either resolved or able to be resolved within the near future.

VI. USMC Operational Maneuver from the Sea

The Marine corps C4I architecture for the years 2010 and beyond is outlined in the Draft Marine Corps Operational Maneuver from the Sea Communications architecture. The architecture relies upon a hierarchy of networks with redundant links in order to provide reliable, light weight communications to Marine Corps forces.

The base of the Marine Corps network is the wireless LAN’s (WLAN) that are established at the Battalion level. The wireless LAN’s envision using the JTRS as their backbone and the access point or gateway into the Marine Air Ground Task Force (MAGTF) WAN. The architecture envisions utilizing terrestrial links between the elements of a Battalion, with a satellite based broadcast service for echelons at Battalion and above.

The architecture realizes that a significant portion of the network traffic in a combat configuration is either broadcast or multicast traffic. Orders, overlays and situation updates from headquarters to subordinate units are normally sent from a headquarters to multiple subordinates, and are usually represented by large volumes of data. The OMFTS architecture recognizes this requirement and includes a MAGTF headquarters injection point to a satellite feed that in turn could broadcast to all subordinate stations with a high speed downlink only transmission. This would leave the terrestrial link free for Command and control and situational awareness data and avoid overstressing the limited bandwidths available on the terrestrial links.[45] Much of this data would be utilized by the battalion and larger Combat Operations Centers (COC).

The Combat Operations Center needs to be mobile and rapidly deployable in order to support the OMFTS concept. The communications architecture envisions vehicle mounted COC modules each equipped with a wireless LAN transceiver. As soon as two COC modules were activated within line of site of each other they would immediately establish LAN connectivity and be able to operate rapidly. This would enable the COC to transmit data internally without the normal long setup times and equipment overhead required to lay cable and connect wires. It would also allow the modules to each operate in their respective networks and share data between each other thus reducing the number of radios required for the entire COC but allowing anyone in the COC to access whichever network they required for their function.[46]

The architecture envisions a minimization of the number of stovepipes in use. It does envision a limited number of stovepipes for specialized applications such as sensor links where an extremely high degree of Low Probability of Intercept (LPI) / Low Probability of Detection (LPD) is required due to proximity of or in enemy controlled areas.

Operational Maneuver from the Sea clearly recognizes the need for the future Marine Corps network to be self configuring and self organizing in order to reduce the overhead currently required for communications personal in a MAGTF. It also recognizes that in order to accomplish this objective the JTRS will have to use routing protocols that are substantially different from those being pursued in the commercial market.[47] This will cause a lower degree of standards compliance.

The network will use COTS components where it is feasible. The COC WLAN envisions the use of some form of limited distance broadband wireless transceiver. There are several versions of these already available on the commercial market and more are sure to follow. The primary unique requirement for the Marine COC would be the introduction of a Communications Security (COMSEC) capability to prevent the interception of traffic between the COC shelters.

While the Operational Maneuver from the Sea Architecture recognizes the need for security it appears to rely upon the components of the network to provide the security capability, rather than including that as an architecture feature.[48]

VII. Ricochet Micro Cellular Data Network

The Ricochet Micro Cellular Data Network is a commercial solution to providing internet connectivity to Mobile users. In the Ricochet Network transceivers are mounted on the top of utility poles and communicate with each other at a data rate of 77 kb/s using spread spectrum technology. A mobile user has a wireless modem installed in his PC or laptop which can then communicate with one of the pole top transceivers or with each other at a maximum data rate of 38.4 kb/s.[49]

This system appears to provide much of the flexibility and adaptability required by the Army After Next. The pole mounted transceivers communicate with each other using the same kind of spread spectrum technology as the PC modem transceivers. The only relatively inflexible component of the system is the router that is used to provide access to the internet. The router link would be a potential single point of failure in the overall network. It is important to note that any station within a network could still communicate with each other even if the gateway point was non operational. A second significant limitation of the system is that the pole mounted radios maintain tables of which modems are communicating with it. Because of the limited range of the radios (about one mile) if a modem is moving faster than about 10 miles per hour the network tends to lose track of the modem.[50] This could be a serious problem for the mobile forces of Army After Next unless either the power levels were increased or a better way to handle the modem tables was developed. The PC mounted modems are about the size of a TV remote control and would be suitable for dismounted soldiers without adding significant weight. Because the PC modems are of small size and relatively low cost they could also be utilized in situations where the establishment of a wireless LAN is desired without establishing a full tactical internet.[51]

The system relies upon the use of spread spectrum transmission technology to provide for transmission security. While spread spectrum does provide for low probability of intercept / low probability of detection (LPI/LPD) it is not invulnerable to interception. In order to be suitable for use in a tactical environment as a classified network an NSA endorsed encryption capability would have to be added at some point in the network. With the current advances in software based encryption and miniaturization of components the capability should not significantly increase the size or weight of the transceivers. In their current configuration they do not meet the Army security profile for the Army After Next.

This system has a marked advantage over other technologies in that it is not only relatively mature, but it is deployed now in a commercial environment where there is a financial incentive for continual improvements and enhancements to the network. It is not unreasonable to predict that the data rates will probably increase with time, the transceivers will become smaller and the ability of the receiver modem to move at higher speeds will be developed to meet commercial market demands.[52]

The bandwidth of the currently available versions compares quite favorably with the tactical internet currently in use by Force XXI. Each of the pole mounted transceivers communicate with each other at a data rate of 77 kb/s and each of the radio modems has a maximum data rate of 38.4 kb/s.[53] the only significant limitation is that depending on how many links are available to the internet gateway a situation could develop where all of the radio modems are sharing a single 77 kb/s radio link to the gateway point. While this would require the gateway operator to monitor the status of his transceiver this should be avoidable in most operational situations.

Ricochet wireless networks offers a commercial alternative to the technologies under development that has a demonstrated potential to be adaptable to the needs of the army after next. If the primary weaknesses of being unable to operate with fast moving nodes and lack of robust security can be overcome it would provide an opportunity to leverage a COTS solution at significant cost savings.

VIII. Cellular Digital Packet Data

Cellular Digital Packet Data (CDPD) is a commercial technology based on the widely deployed commercial cellular telephone networks. It uses the existing 30 KHz voice channels of the cellular network to provide data at up to 19.2 kb/s.

Because CDPD rides over existing analog cellular telephone network it largely benefits and suffers from cellular telephones capabilities and limitations. The cellular network is designed to be a static series of towers or “cells” which communicate with mobile subscribers. These cells each have to perform intelligent management functions and reconfiguring these cells is both difficult and time consuming. However, because all of the management and nearly all of the intelligence resides in the cells the system is relatively simple from a subscribers point of view.

Security is a significant issue with analog cellular networks and CDPD suffers from similar problems. It is a fixed channel 30 KHz application that operates in a fixed spectrum, this makes the signal very vulnerable to interception, jamming, imitative deception, spoofing and any other number of electromagnetic warfare techniques. Because of its higher frequency range it is also possible to very precisely determine the azimuth to any operating device. While encryption of the data stream could conceivably mitigate the interception and monitoring problems the system design prohibits the resolution of the jamming and position location problems.

The CDPD network was also designed and optimized for data messages of very short length (less than 600 words) and does not perform well under large data loads.[54] This makes it particularly unsuitable for applications with large data loads such as video teleconferencing. Indications are that even though the nominal bandwidth is 19.2 kb/s the actual throughput is closer to 9.6 kb/s because of error correction overhead.[55]

IX. Conclusions

As America’s Army moves forward to the Army After Next the need for reliable and robust data communications underpins the gains in knowledge and speed promised by the Army After Next. As more “digitized” systems are fielded the volume of data flowing across the information grid will increase substantially. Commanders will be able to see themselves and see the battlefield as never before. In order to defeat any potential adversaries they must have the best possible communications systems to provide the data when and where it is needed.

The Army After Next is based on “Knowledge and Speed”[56]. In order to support a dynamic battlefield with rapidly moving systems and units the underlying communications system must also be highly adaptable, able to rapidly adjust to the entry and exit of communications devices from the network with a minimum of operator intervention.

The Army’s Current Architecture for the Tactical Internet clearly does not meet this requirement. With a twelve to twenty-four hour requirement to reconfigure the network to support a change in task organization the network cannot respond to rapid changes in the battlefield. Further the process of reconfiguring the network is strictly a manual, labor intensive process. Both the high manpower needs and the inability to adapt mean that their is a need for substantial change as the Army moves to 2025.

The Joint Tactical Radio System is being designed to support a mobile changing network configuration. With a stated requirement to be able to automatically reconfigure its network within 15 minutes the network meets the requirement to be able to adapt rapidly to the movement of systems about the battlefield. The JTRS also adds an additional dimension to adaptability in that it is designed to operate in multiple frequency ranges and waveforms with only software changes. Therefore a JTRS radio could potentially monitor a VHF and microwave network simultaneously, and connect to a Low Orbit Satellite based network. This multinetwork capability increases the adaptability and flexibility of the overall system.

The Navy's MONET system also scores poorly in terms of adaptability. The system is designed to support a fairly static fleet configuration and does not possess the requirement to support a large number of nodes in constant motion. This limits its ability to support lower force echelons which will have a large number of systems rapidly changing geographic areas.

Since the Marine Corps Operational Maneuver from the Sea is also based upon the JTRS it carries the same strengths for adaptability. The software reprogramable capabilities of the JTRS should provide the MAGTF the capability to communicate with both the fleet and units ashore.

Ricochet provides a COTS system which has the needed adaptability to support a dynamic environment envisioned in the Army After Next. Its ability to self organize and recognize nodes in the network makes it a significant player in the AAN architecture. As a contrast the other commercial technology examined, CDPD lacks the flexibility to handle rapid changes and reconfigurations. While it is quite mature the CDPD architecture is simply to rigid to support the requirements of the future battlefield.

Security is also a strength of the JTRS network. Utilizing embedded communications security (COMSEC) devices coupled with LPI/LPD waveforms provides a high degree of communications security. Further the network portion of the JTRS is required to have embedded support for IP security (IPSEC) and eventual support for multi level security. This provides a very strong security architecture for the JTRS network. The current Force XXI architecture also utilizes the embedded COMSEC devices and Frequency Hopping capabilities of the SINCGARS SIP radios to provide link security. However, the current Force XXI architecture lacks any form of network security and the SINCGARS lacks remote lockout capability, so potentially if a SINCGARS node in the network was compromised the entire network becomes vulnerable to compromise.

The Navy MONET network relies upon link security and does not implement any form of IPSEC. However, because MONET is an ATM cell based architecture as the KG-195 series of cell encryptors is fielded the MONET network can implement end to end cell encryption which should significantly enhance the overall security of the network.

Of the commercial alternatives the Ricochet network provides the best security profile since it is using low power spread spectrum techniques to provide link security. However, it lacks actual link encryption or any form of IPSEC therefore once the signal is penetrated the network is vulnerable to intrusion or monitoring.

The most technologically mature networks are the two commercial alternatives. CDPD has been around since 1994 and is widely available throughout the United States. Ricochet has only been implemented in a limited number of cities, but is robust and mature in the areas where it has been installed.

The Army Force XXI system is generally based on available technologies, but a number of Surrogates have had to gradually be removed from the network as the system matures. Further the network continues to lack strong management capabilities and requires considerable further work and maturity to become a robust and reliable network.

The Navy’s MONET system utilizes commercially available technologies however the ATM standards are still relatively new, especially in the constant bit rate (CBR) and voice over ATM areas and the standards are still emerging. As the

ATM standards mature MONET will reach technological maturity.

The JTRS network is still essentially a concept with the second round of proposals due in November 1999. Therefore the maturity of this network is clearly lacking and leaves open the question of whether the JTRS can achieve all of its stated goals or whether the initial radios will be a compromise in order to get the system fielded.

The Navy’s MONET system is the Bandwidth leader of the systems examined, providing a T-1 (1.544 Mb/s) capability or better as a basic link standard. The superior bandwidth performance is clearly a strong benefit of the MONET network.

The Ricochet network also provides superior bandwidth performance with its 77 kb/s link speed or 38.4 kb/s data rate for handheld units. This data rate is superior to most of the systems currently in use for situational awareness. The JTRS is far behind with a data rate of 19.2 kb/s for portable systems. As has been demonstrated during various experiments this does not permit the timely updating of complex graphics and overlays to the lowest level possible and will need to be improved as the JTRS matures.

Finally the current Force XXI architecture and the CDPD share the bottom end data rate of 9.6 kb/s. This data rate is a significant limitation on the ability to maintain situational awareness updated and to distribute new orders and information as operations evolve.

The Joint Tactical Radio System is clearly the path to the future for the Army and for Joint forces as they proceed to full digitization. Its strengths in adaptability and security make it the preferred system for the Army After Next. The Army must examine the technologies present in the Ricochet system for inclusion as part of the JTRS architecture in order to improve the bandwidth available in the JTRS network. Increasing the available bandwidth will improve its ability to move the volumes of data required by the warfighter and improve its ability to pass the management data required to rapidly reconfigure the network as nodes enter and leave the network.

The Navy’s MONET system is far too rigid to serve in the fast moving environment at echelon’s Brigade and below, however its superior bandwidth capabilities make it a system that should be seriously considered for applications linking major headquarters and linking joint force headquarters to support high bandwidth requirements such as imagery, video and large volumes of data traffic.

Since the Marine network is primarily a linking of JTRS and MONET it meets the standards of the networks discussed above and represents an ideal architecture for all Joint Land Forces in 2010 and beyond.

X. ENDNOTES

[1] US Army, United States Army Training and Doctrine Command, Knowledge and Speed: Battle Force and the U.S. Army of 2025. (Fort Monroe, Virginia: US Government Printing Office, 7 December 1998) p. 9.

[2] Paul T. Hengst "Managing the Intelligent Information Grid for the Army After Next" AY 97 Compendium Army After Next Project (Strategic Studies Institute, Carlisle PA 6 April 1998)p 111.

[3] Knowledge and Speed: Battle Force and the U.S. Army of 2025 pp. 9-10, 14.

[4] Force XXI uses a mix of modified versions of currently fielded equipment to achieve the required data connectivity. The data radio, SINCGARS - SIP, is a modified version of the fielded SINCGARS ICOM radios which had a better data modem installed to provide more reliable data transmission at 9600 bits per second. The Enhanced Position and Locating Reporting System (EPLRS) has been under design in various forms since the 1970's and was envisioned primarily as a position locating tool until the advent of GPS made the positioning capability less relevant. However, the EPLRS - VHSIC version proved to be a superb data radio and was drafter to function as a data radio instead of a position reporting tool. Mobile Subscriber Equipment (MSE) has been enhanced with the addition of the High Speed Multiplex (HSMUX) equipment in order to facilitate data transmission at up to 512 Kb/s. The only system designed specifically for Force XXI is the Near Term Digital Radio (NTDR) and its predecessor the Surrogate Digital Radio (SDR) which were designed specifically to provide high speed data links between Brigade TOC's. Because of the challenges and high degree of technical skills required to manage these systems one of the most consistent features of all of the Advanced Warfighting Experiments have been the small armies of contractors required to manage and support these systems.

[5] The Defense Information Systems Agency (DISA) utilizes nearly all commercial equipment for its Defense Information Systems Network (DISN). Most U.S. Army Theater Signal Commands utilizes commercial equipment for strategic communications, and a large variety of COTS equipment to provide increased capabilities over the standard tactical equipment.

[6] Dr. Earl H. Tilford, Jr., ed., Strategic Challenges in an Uncertain World. (Strategic Studies Institute Carlisle Barracks, PA, 5 February 1996) p. 5.

[7] William T. Lasher, "Data Interoperability for Systems of Systems: Our acquisition Paradigm Must Change to Achieve It", AY 97 Compendium Army After Next Project (Strategic Studies Institute, Carlisle Barracks, PA 6 April 1998) pp. 136-138.

[8] US Army Joint Technical Architecture - Army Version 5.5 (Washington DC 23 December 1998) p.1.

[9] US Army Training and Doctrine Command Knowledge and Speed: Battle Force and the U.S. Army of 2025 (Fort Monroe VA 7 December 1998) pp 9-10.

[10] Steve Steinke Guide to Managing PC Networks (Prentice Hall, Englewood Cliffs NJ 1995) p. 222.

[11] Knowledge and Speed: Battle Force and the U.S. Army of 2025, pp 9-10.

[12] Joint Technical Architecture - Army, p. 63.

[13] Ibid., pp 63-64.

[14] William Stallings Cryptography and Network Security: Principles and Practice Second Edition (Prentice Hall, Upper Saddle River NJ 1999), pp 9-11.

[15] To provide some idea of how bits per second relates to data carrying capacity, the latest modems currently on the market operate 56,000 bits per second or 56 kb/s. A single phone call on modern telephone switch requires 64,000 bits per second to accurately reproduce the sound of the conversation.

[16] US Army, Force of Decision ...Capabilities for the 21st Century. (Washington DC 15 April 1996).

[17] US Army Training and Doctrine Command, Land Combat in the 21st Century. (Fort Monroe VA 1996) pp. 18-19.

[18] TRADOC PAM 525, p. 1-5.

[19] FM 24-32 (draft version 5 October 1997), pp 1-1, 1-3.

[20] TRADOC Systems Manager for tactical Radio, “Tactical Radio, Tactical Internet Mature for Task Force XXI and beyond”, Army Communicator, Summer 97, Vol. 22 Issue 3 pp 21-24.

[21] Ibid., pp 23-24.

[22] Captain Michael D. Brady “Intelligence Operations on the Digitized Battlefield” Military Intelligence Professional Bulletin, Jul-Sep97, Vol. 23 Issue 3, p23-25.

[23] TRADOC Systems Manager for tactical Radio, “Tactical Radio, Tactical Internet Mature for Task Force XXI and beyond”, Army Communicator, Summer 97, Vol. 22 Issue 3 pp 21-24.

[24] Major Robert Casper, Mobile Subscriber Equipment, briefing to US Army Command and General Staff College, Advanced Communications Elective, Academic Year 1998-1999, slide 36.

[25] The heavy use of CISCO routers and the Open Shortest Path First (OSPF) internal routing protocol contributes greatly to this problem. The OSPF protocol does not permit dynamic reassignment of IP subnets between networks without significant management effort and overhead. Also the static nature of the EPLRS network contributes to these difficulties.

[26] SFC Tim Leandreth and Jackie Watkins “Team Signal Improves Tactical Internet for Force XXI” Army Communicator Summer 97 Vol. 22 Issue 3 pp 19-20.

[27] Brady, pp 23-25.

[28] FM 24-32, pp 14-1 - 14-8.

[29] Joint Tactical Radio System Joint Program Office “JTRS Explained” available from http://www.jtrs.sarda army.mil/explain/index.html; Internet; accessed 10 October 1999.

[30] JTRS Joint Program Office Operational Requirements Document (ORD) for Joint Tactical Radio (JTR) (Washington DC 23 March 1998) Available at http://www.dtic.mil/jcs/j6/jtr23_mar.html; Internet; accessed on 11 October 1999, pp 15-17.

[31] Ibid. pp 12-13.

[32] Ibid. p 5.

[33] Office of the Joint Chiefs, J6 Command, Control, Communications and Computers Systems (C4S) directorate Mission Needs Statement (MNS) for the Joint Tactical Radio (JTR) (Washington DC 21 August 1997) Available from http://www.dtic.mil/jcs/j6/mns_21aug.html; Internet; accessed on 11 October 1999).

[34] Operational Requirements Document for Joint Tactical Radio p.8. In addition the objective radio version, scheduled for FY-05 requires the capability to act as a gateway for cell switched networks.

[35] SFC Tim Leandreth and Jackie Watkins “Team Signal Improves Tactical Internet for Force XXI” Army Communicator Summer 97 Vol. 22 Issue 3 pp 19-20.

[36] TRADOC Systems Manager Tactical Radio, “Joint Tactical Radio System (JTRS) Operational Concept (Army Perspective)” August 1999 available at http://www.gordon.army.mil/tsmtr/jtrfact.ppt ; Internet; accessed on 8 October 1999.

[37] N.P. Newman, T. Stiller, and W.E. Stephens Joint Adaptive Communications System (JACS) Concept Validation Study (Rome Laboratory Air Force Material Command, Rome NY July 1997) p 31.

[38] Ibid., pp 23-24.

[39] Joint Technical Architecture - Army, pp 6-9.

[40] Dr. Clifford J. Warner and Dr. Nickhill Davé, “Monet - The High Data Rate MObile interNET” AFSEA C4I Symposium Proceedings April 1994, pp.-2.

[41] Ibid. p 6.

[42] Joint Technical Architecture - Army pp 38-45.

[43] Warner, et al, pg 5. Based on the authors discussion it appears the bridges were also capable of Layer 3 routing but were used in a Layer 2 (bridging) mode.

[44] Hengst, pg 114.

[45] Lieutenant Colonel M. E. Cantrell, Overview of the Draft Marine Corps Operational Maneuver from the Sea Communications Architecture (Marine Corps Combat Develop Command, Quantico VA 1999). pp 4-5.

[46] Ibid. p. 4.

[47] Ibid. p. 1.

[48] Ibid. p.1.

[49] Kieran M. Taylor, “Big Bandwdith Small Cities” Data Communications August 1994 pp. 95-97.

[50] Ibid. p 97.

[51] Ibid. pp 95-96.

[52] “Metricom Hits High-Speed Milestone; Exits Beta Testing” Metricom Press Release, 21 July 1999, available at http://www.metricom.com/journalists/news/news990721.htm, accessed on 12 November 1999. Metricom announced that it will deploy its 128 kb/s service in Calendar Year 2000. The current Ricochet modems have also decreased from the original modem at 14 ounces to the Ricochet SE at 10 ounces.

[53] Ibid. pp 95-96.

[54] U.S. Congress, Office of Technology Assessment, Wireless Technologies and the National Information Infrastructure, OTA-ITC-622 (Washington DC: U.S. Government Printing Office, July 1995) p 112.

[55] Ibid. p.112.

[56] Knowledge and Speed: Battle Force and the U.S. Army of 2025 p 9.

BIBLIOGRAPHY

BOOKS

Bates, Regis J. Wireless Networked Communications Concepts, Technology, and Implementation New York: McGraw-Hill, Inc. 1994.

Kadambi, Jayant, Ian Crayford, Mohan Kalkunte Gigabit Ethernet Upper Saddle River NJ: Prentice Hall 1998.

Simonds, Fred Network Security: data and voice communications. New York: McGraw-Hill, 1996.

Stallings, William Cryptogrpahy and Network Security: Principles and Practice. Upper Saddle River NJ: Prentice Hall 1998.

Steinke, Steve Guide to Managing PC Networks. Englewood Cliffs, NJ: Prentice-Hall, Inc. 1995.

Tanenbaum, Andrew Computer Networks. Englewood Cliffs, NJ: Prentice-Hall, Inc. 1996.

MONOGRAPHS, STUDENT ESSAYS, STUDY PROJECTS AND THESES

Cantrell, Lieutenant Colonel M. E. Overview of the Draft Marine Corps Operational Maneuver from the Sea Communications Architecture Quantico VA: Marine Corps Combat Development Command 1999.

Hall, Major W. Russell, Battle Command: Tactical Decision-Making in the Information Age. Fort Leavenworth KS: US Army Command and General Staff College School of Advanced Military Studies December 1996.

Johnson, Douglas V., editor. AY 97 compendium Army After Next Project. Carlisle Barracks, PA: Strategic Studies Institute, 1998.

Tilford, Dr. Earl H., editor. Strategic Challenges in an Uncertain World. Carlisle Barracks, PA: Strategic Studies Institute, 1996.

MAGAZINES, ARTICLES AND PERODICALS

Blair, Captain Obediah “Update on Tactical Internet and Force XXI Battle-Command for Brigade and Below” Army Communicator, Summer 1998, Vol. 23 Issue 3, pp20-23.

Brady, Captain Michael D. “Intelligence Operations on the Digitized Battlefield” Military Intelligence Professional Bulletin, Jul-Sep 1997, Vol 23 Issue 3, p23-25.

Hanna, Mark “Task Force XXI: The Army’s Digital Experiment” National Defense University Strategic Forum, Institute for Strategic Studies Number 119, July 1997, internet: http://www.ndu.edu/inss/strforum/forum119.html accessed on 5 August 1999.

Landreth, SFC Tim and Jackie Watkins “Team Signal Improves TActical Internet for Force XXI” Army Communicator, Summer 1997, Vol 22 Issue 3, p19-20.

“Metricom Hits High-Speed Milestone; Exits Beta Testing” Metricom Press Release, 21 July 1999, internet: http://www.metricom.com/journalists/news/news990721.htm accessed on 12 November 1999.

Taylor, Kieran M. “Big Bandwidth, Small Cities” Data Communications, August 1994 pp95-97.

US Army Training and Doctrine Command systems manager for tactical radio “Tactical Radio, Tactical Internet Mature for Task Force XXI and Beyond” Army Communicator, Summer 1997, Vol 22 Issue 3, pp 21-24.

MILITARY MANUALS, PUBLICATIONS AND GOVERNMENT DOCUMENTS

Congress of the United States General Accounting Office, Battlefield Automation: Acquisition Issues Facing the Army Battle Command, Brigade and Below Program. GA/NSIAD-98-140 Wahsington DC: U.S. Government Printing Office, 30 June 1998.

Congress of the United States Office of Technology Assesment, Wireless Technologies and the National Information Infrastructure. OTA-ITC-622 Washington DC: U. S. Government Printing Office, July 1995.

Department of the Army, Force of Decision ...Capabilities for the 21st Century April 1996.

Department of the Army Joint Technical Architecture - Army (JTA-Army) v5.5 Washington DC: Office of the Director for Information Systems, Command, Control, Communications and Computers, 23 December 1998, Internet http://arch-odisc4.army.mil/ades/aea/jta-a/jtaa55/html/jtaa55.htm accessed on Aug 29 1999.

Headquarters, United States Army Training and Doctrine Command TRADOC Pamphlet 525-5: Force XXI Operations. Fort Monroe VA 1 August 1994.

Headquarters, United States Army Training and Doctrine Command Knowledge and Speed: Battle Force and the U.S. Army of 2025. December 1998.

Headquarters, United States Army Training and Doctrine Command Land Combat in the 21st Century 1996.

Jont Tactical Radio System Joint Program Office, JTRS Explained 19 August 1999 availbe from http://www.jtrs.sarda.army.mil/explain/index.html, Internet, accessed on 10 October 1999.